Foundation of Cryptography (0368-4162-01), Intoduction

Adminstration + Introduction

Iftach Haitner, Tel Aviv University

Tel Aviv University.

February 26, 2013

Part I

Administration and Course Overview

Section 1

Administration

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
2. Who are you?

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
2. Who are you?
3. Mailing list: 0368-4162-01@listserv.tau.ac.il

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
2. Who are you?
3. Mailing list: 0368-4162-01@listserv.tau.ac.il
   - Registered students are automatically on the list (need to activate the account by going to `https://www.tau.ac.il/newuser/`)

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
2. Who are you?
3. Mailing list: 0368-4162-01@listserv.tau.ac.il
   - Registered students are automatically on the list (need to activate the account by going to `https://www.tau.ac.il/newuser/`)
   - If you're not registered and want to get on the list (or want to get another address on the list), send e-mail to: listserv@listserv.tau.ac.il with the line:
     subscribe 0368-3500-34 <Real Name>

Important Details

1. Iftach Haitner. Schriber 20, email iftachh at gmail.com
   Reception: Sundays 9:00-10:00 (please coordinate via email in advance)
2. Who are you?
3. Mailing list: 0368-4162-01@listserv.tau.ac.il
   - Registered students are automatically on the list (need to activate the account by going to `https://www.tau.ac.il/newuser/`)
   - If you're not registered and want to get on the list (or want to get another address on the list), send e-mail to: listserv@listserv.tau.ac.il with the line:
     subscribe 0368-3500-34 <Real Name>
4. Course website:
   `http://www.cs.tau.ac.il/~iftachh/Courses/FOC/Spring13`
   (or just Google iftach and follow the link)

Grades

1. Class exam 80

Grades

1. Class exam 80
2. Homework 20%: 5-6 exercises.

Grades

1. Class exam 80
2. Homework 20%: 5-6 exercises.
   - Recommended to use use LaTex (see link in course website)

Grades

1. Class exam 80
2. Homework 20%: 5-6 exercises.
   - Recommended to use use LaTex (see link in course website)
   - Exercises should be sent to ? or put in mailbox ?, in time!

and..

1. Slides

and..

1. Slides
2. English

Course Prerequisites

1. Some prior knowledge of cryptography (such as 0369.3049) might help, but not necessarily
2. Basic probability.
3. Basic complexity (the classes $\mathcal{P}$, $\mathcal{NP}$, $\mathcal{BPP}$)

Course Material

1. Books:
   1. Oded Goldreich. Foundations of Cryptography.
   2. Jonathan Katz and Yehuda Lindell. An Introduction to Modern Cryptography.
2. Lecture notes
   1. 2011 Course.
   2. Ran Canetti. Foundation of Cryptography (The 2008 course)
   3. Salil Vadhan. Introduction to Cryptography.
   4. Luca Trevisan. Cryptography.
   5. Yehuda lindell Foundations of Cryptography.

Section 2

Course Topics

Course Topics

Basic primitives in cryptography (i.e., one-way functions, pseudorandom generators and zero-knowledge proofs).

- Focus on *formal* definitions and *rigorous* proofs.
- The goal is not studying some list, but to understand cryptography.
- Get ready to start researching

Part II

Foundation of Cryptography

Cryptography and Computational Hardness

1. What is Cryptography?

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

   $\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

   $\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:

   1. $V(x, w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

   $\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:

   1. $V(x,w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$
   2. for any $x \in L$, $\exists w \in \{0,1\}^*$ with $|w| \leq p(|x|)$ and $V(x,w) = 1$

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

$\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:

1. $V(x,w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$
2. for any $x \in L$, $\exists w \in \{0,1\}^*$ with $|w| \leq p(|x|)$ and $V(x,w) = 1$

$\mathcal{P} \neq \mathcal{NP}$: i.e., $\exists L \in \mathcal{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $A(x) \neq 1_L(x)$

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

$\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:

1. $V(x,w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$
2. for any $x \in L$, $\exists w \in \{0,1\}^*$ with $|w| \leq p(|x|)$ and $V(x,w) = 1$

$\mathcal{P} \neq \mathcal{NP}$: i.e., $\exists L \in \mathcal{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $A(x) \neq 1_L(x)$

polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in \text{poly}$ such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

   $\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:
   1. $V(x,w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$
   2. for any $x \in L$, $\exists w \in \{0,1\}^*$ with $|w| \leq p(|x|)$ and $V(x,w) = 1$

   $\mathcal{P} \neq \mathcal{NP}$: i.e., $\exists L \in \mathcal{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $A(x) \neq 1_L(x)$

   polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in \text{poly}$ such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$
4. Problems: hard on the average. No known solution

Cryptography and Computational Hardness

1. What is Cryptography?
2. Hardness assumptions, why do we need them?
3. Does $\mathcal{P} \neq \mathcal{NP}$ suffice?

   $\mathcal{NP}$: all (languages) $L \subset \{0,1\}^*$ for which there exists a polynomial-time algorithm V and (a polynomial) $p \in \text{poly}$ such that the following hold:
   1. $V(x,w) = 0$ for any $x \notin L$ and $w \in \{0,1\}^*$
   2. for any $x \in L$, $\exists w \in \{0,1\}^*$ with $|w| \leq p(|x|)$ and $V(x,w) = 1$

   $\mathcal{P} \neq \mathcal{NP}$: i.e., $\exists L \in \mathcal{NP}$, such that for any polynomial-time algorithm A, $\exists x \in \{0,1\}^*$ with $A(x) \neq 1_L(x)$

   polynomial-time algorithms: an algorithm A runs in polynomial-time, if $\exists p \in \text{poly}$ such that the running time of $A(x)$ is bounded by $p(|x|)$ for any $x \in \{0,1\}^*$
4. Problems: hard on the average. No known solution
5. One-way functions: an efficiently computable function that no efficient algorithm can invert.